UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/524,358	03/14/2000	Tateo Oishi	450100-02402	8951

20999   7590   01/27/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER
NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/524,358	OISHI ET AL.
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _06 October 2004_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-6 and 8-18_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-6, 8-18_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _14 March 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____ .

U.S. Patent and Trademark Office
PTOL-326 (Rev. 1-04)   Office Action Summary   Part of Paper No./Mail Date 20050119

DETAILED ACTION

1.   Claims 1-6 and 8-18 are pending.

2.   Amendment submitted 6 October 2004 has been received and entered.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-6 and 8-18 have been considered

but are not persuasive.

4.   Applicant has argued on page 9 that the combination of Schneier and Sasaki

fails to teach expanding compressed data in units that are a multiple of the length of an

encryption block.   Examiner respectfully disagrees. Examiner contends that Schneier

does teach the above-cited limitation by teaching an expansion permutation that

expands data from 32 bits to 48 bits (Schneier, page 273) where 48 bits is a multiple of

an encryption block size of 8.

5.   Applicant has argued on page 12 that the combination of Sasaki, Bellovin,

Cassagnol, and Yuenyongsgool fails to teach control means that "stores said one or

more processing blocks at consecutive addresses of said storage means in the order of

encryption." Applicant has focused on the lack of teaching for the emphasized

limitation, "in the order of encryption." Examiner respectfully disagrees. Examiner has

relied upon Yuenyongsgool to teach the storing of processing blocks at consecutive

addresses (Yuenyongsgool, column 2, lines 38-45). Examiner contends that Sasaki

teaches the storing of processing blocks in the order of encryption (Sasaki, Figure 8,

Items S72, S73, S74).

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1, 6, and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by

Bruce Schneier's Applied Cryptography in view of Sasaki et al US Patent No.

6,378,071. Schneier teaches the implementation of the DES algorithm. Sasaki teaches

a file access system for encrypted data within a storage device.

8.   With regards to claims 1 and 13, Schneier discloses processing means for

defining a processing block having a data block length of a whole multiple of the

predetermined length of an encryption block and for expanding compressed data in

units of the predetermined processing block length (Schneier, Page 273, Expansion

Permutation, Page 270, Section 12.2 "Outline of the Algorithm", Processing Block

viewed as 64 bit block, encryption block viewed as a byte), and a control means for

writing encrypted data so that data positioned in the same encryption block is also

positioned in the same processing block (Schneier, Page 271, Figure 12.1). Schneier

fails to teach a storage means for storing encrypted data. Sasaki teaches a storage

means for storing encrypted data (Sasaki, column 3 lines 35-37 and column 4 lines 4-6).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to include Sasaki's storage means because it offers the advantage of providing a simple accessing method for efficiently accessing a file within an external storage device and provides security for file information (Sasaki, column 1 lines 52-62).

9.   With regards to claim 6, Schneier as modified teaches the control means outputting data read out into the processing means (Sasaki, column 3 lines 14-16).

10.   Claims 2-3, 14-15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography and Sasaki et al US Patent No. 6,378,071, as applied to claims 1 and 13 above, and in further view of Bellovin et al US Patent No. 5,241,599.

11.   With regards to claims 2 and 14, Schneier and Sasaki as described above fail to teach the inserting of data into the processing block in order to adjust the data length so that it becomes a whole number multiple of the predetermined length. Bellovin teaches the insertion of data in order to meet the predetermined length of a block (Bellovin, column 10, lines 24-30). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bellovin's method of inserting data because it offers the advantage of helps prevent partition attacks against encryption keys (Bellovin, column 9 line 54 – column 10 line 47).

12.   With regards to claims 3, 15, and 18, Schneier and Sasaki fail to teach the encryption process using the block to be encrypted and a ciphertext from the previous block. Bellovin teaches an encryption process using the block to be encrypted and a

ciphertext from the previous block in the form of cipher-block chaining (Bellovin, column

13, lines 10-13 and 30-35).

13.   Claims 4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Schneier Applied Cryptography, Sasaki et al US Patent No. 6,378,071, and Bellovin et

al US Patent No. 5,241,599 as applied to claims 3 and 15 above, and further in view of

Cassagnol US Patent No. 6,385,727. Schneier, Sasaki, and Bellovin, teach a cluster of

encrypted data stored in a storage means (Sasaki, column 3, lines 52-55, "file"), but fail

to teach the storing of values initially used when encrypting stored in one of the

processing blocks. Cassagnol teaches the storing of values initially used (cited as

whitening keys) when encrypting stored in one of the processing blocks (Cassagnol,

column 10, lines 37-52). At the time the invention was made, it would have been

obvious to a person of ordinary skill in the art to utilize Cassagnol's method of storing

initial values because it offers the advantage of allowing keys to be stored with and thus

imported with their respective encrypted blocks (Cassagnol, column 10, lines 49-52)

and helps preserve memory resources by reducing the need for on chip memory

storage of keys (Cassagnol, column 10, lines 40-47).

14.   Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Schneier Applied Cryptography, Sasaki et al US Patent No. 6,378,071, Bellovin et al US

Patent No. 5,241,599, and Cassagnol US Patent No. 6,385,727 as applied to claim 4

above, and further in view of Yuenyongsgool US Patent No. 6,202,152. Schneier,

Sasaki, Bellovin, and Cassagnol, as described above, teach the storing of processing

blocks in the order of encryption (Sasaki, Figure 8, Items S72, S73, S74), but fail to

teach the storage of blocks at consecutive addresses. Yuenyongsgool teaches the

storage of data by consecutive addresses (Yuenyongsgool, column 2, lines 38-45,). At

the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to utilize Yuenyongsgool's method of consecutive address storage

because it offers the advantage of helping accelerate information transfers from

encrypted memory (Yuenyongsgool, column 2, lines 4-23).

15.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier

Applied Cryptography in view of Sasaki et al US Patent No. 6,378 and Bahout et al US

Patent No. 5,594,793. Schneier and Sasaki, as described above with regards to claim

1, fail to teach a system for mutual identification between the storage and data

processing apparatuses. Bahout teaches a system for mutual identification between the

storage and data processing apparatuses using stored keys and algorithms within the

data processor (Bahout, column 7, lines 7-25). At the time the invention was made, it

would have been obvious to a person of ordinary skill in the art to utilize Bahout's

mutual identification method because it offers the advantage of giving the system a

degree of inviolability by ensuring that data processor only functions with a specific

storage device (Bahout, column 1, lines 9-16 and 55-60).

16.   Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Schneier Applied Cryptography, Sasaki et al US Patent No. 6,378,071, and Bahout et al

US Patent No. 5,594,793, as applied to claim 8 above, and in further view of Bellovin et

al US Patent No. 5,241,599.

17.   With regards to claim 9, Schneier, Sasaki, and Bahout, as described above fail to

teach the inserting of data into the processing block in order to adjust the data length so

that it becomes a whole number multiple of the predetermined length. Bellovin teaches

the insertion of data in order to meet the predetermined length of a block (Bellovin,

column 10, lines 24-30). At the time the invention was made, it would have been

obvious to a person of ordinary skill in the art to utilize Bellovin's method of inserting

data because it offers the advantage of helps prevent partition attacks against

encryption keys (Bellovin, column 9 line 54 – column 10 line 47).

18.   With regards to claim 10, Schneier, Sasaki, and Bahout fail to teach the

encryption process using the block to be encrypted and a ciphertext from the previous

block. Bellovin teaches an encryption process using the block to be encrypted and a

ciphertext from the previous block in the form of cipher-block chaining (Bellovin, column

13, lines 10-13 and 30-35).

19.   Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier

Applied Cryptography, Sasaki et al US Patent No. 6,378,071, Bahout et al US Patent

No. 5,594,793, and Bellovin et al US Patent No. 5,241,599 as applied to claim 11

above, and further in view of Cassagnol US Patent No. 6,385,727. Schneier, Sasaki,

Bahout, and Bellovin, teach a cluster of encrypted data stored in a storage means

(Sasaki, column 3, lines 52-55, "file"), but fail to teach the storing of values initially used

when encrypting stored in one of the processing blocks. Cassagnol teaches the storing

of values initially used (cited as whitening keys) when encrypting stored in one of the

processing blocks (Cassagnol, column 10, lines 37-52). At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to utilize

Cassagnol's method of storing initial values because it offers the advantage of allowing

keys to be stored with and thus imported with their respective encrypted blocks

(Cassagnol, column 10, lines 49-52) and helps preserve memory resources by reducing

the need for on chip memory storage of keys (Cassagnol, column 10, lines 40-47).

20.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier

Applied Cryptography, Sasaki et al US Patent No. 6,378,071, Bahout et al US Patent

No. 5,594,793, Bellovin et al US Patent No. 5,241,599, and Cassagnol US Patent No.

6,385,727 as applied to claim 11 above, and further in view of Yuenyongsgool US

Patent No. 6,202,152. Schneier, Sasaki, Bahout, Bellovin, and Cassagnol, as

described above, fail to teach the storage of blocks at consecutive addresses.

Yuenyongsgool teaches the storage of data by consecutive addresses (Yuenyongsgool,

column 2, lines 38-45). At the time the invention was made, it would have been obvious

to a person of ordinary skill in the art to utilize Yuenyongsgool's method of consecutive

address storage because it offers the advantage of helping accelerate information

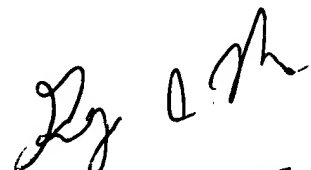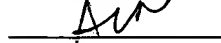transfers from encrypted memory (Yuenyongsgool, column 2, lines 4-23).

Conclusion

21.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Andrew L Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100